Controls and Assurance in the Cloud: Using COBIT 5

Controls and Assurance in the Cloud: Using COBIT® 5 provides comprehensive process practices and a governance framework to use when conducting an assessment of cloud computing, including its associated security risk. This book is a useful resource for those involved in establishing a secure cloud computing environment in their organization. The book is also a necessary resource for IS auditors who are assessing controls and governance arrangements in an organization that is embarking on a cloud computing solution.

As with similar publications, the book explains the fundamentals of cloud computing, including the drivers, cloud service models and risk factors to consider before moving to the cloud. It explains the three different cloud service models (Infrastructure as a Service [IaaS], Platform as a Service [PaaS] and, Software as a Service [SaaS]) and the different deployment models (public, community, private and hybrid cloud). It elaborates on some newer cloud service models, including Identity as a Service, Disaster Recovery as a Service (DRaaS), and Security as a Service.

The book steps through some common cloud computing challenges based on the seven COBIT® 5 enablers:

1. Principles, Policies and Frameworks

2. Processes

3. Organisational Structures

4. Culture, Ethics and Behaviour

5. Information

6. Services, Infrastructure and Applications

7. People, Skills and Competencies.

The book includes a clearly defined risk assessment by cloud service model and by deployment model.

One of the most beneficial chapters of the book is on governance and management in the cloud. This information would be useful for IT managers and other senior executives. This chapter includes targeted questions and considerations about the governance and management of a cloud solution, taking into consideration benefits realization, which can assist in ensuring risk factors are considered and appropriate decisions are made to provide adequate control over the solution once it is in place.

The COBIT 5 Goals Cascade is incorporated into the book, showing links between the enterprise goals and IT goals of an organization down to relevant COBIT 5 processes, which provide a useful framework for managing the cloud by using COBIT 5.

The book's numerous appendices provide the reader with valuable tools for conducting a cloud assurance review and a process capability assessment, and measuring the return on investment on a cloud solution. The appendices also provide cloud risk scenarios and a checklist for the board of directors to work through when considering a decision to move to the cloud.

One of the most valuable appendices in this book is on contractual provisions. This outlines

Reviewed by Diana M. Hamono, CISA, CGEIT, COBIT 5 Foundation
Executive director of the governance, risk and assurance team at Synergy Group in Canberra, Australia, and a past president of the ISACA Canberra Chapter.

important clauses that should exist in contracts with cloud service providers. If these clauses are not incorporated, or at least considered, during contract negotiations, then the organization could put its data at risk, and it could end up in a dispute with the parties involved in the cloud service delivery model.

Controls and Assurance in the Cloud covers all aspects related to the decision to move to a cloud model and provides a range of pertinent questions and points for executives, IT managers, business managers and auditors to consider. It is

a comprehensive and well-organized book that would be of great benefit to IS auditors tasked with assessing cloud computing controls or assessing the risk involved in a move to cloud services.

Editor's Note

Controls and Assurance in the Cloud: Using COBIT® 5 is available from the ISACA® Bookstore. For information, visit *www.isaca.org/bookstore*, contact support at https://support.isaca.org/ or telephone +1.847.660.5650.